REMARKS

Reconsideration of the pending application is respectfully requested on the basis of the following particulars.

1. Priority Document

A certified copy of application No. 10317257.2, filed in Germany, was made of record in this application on September 5, 2006. Applicant respectfully requests the Examiner to indicate on the next Office action that this document has been received and to further acknowledge the priority claim thereto.

2. In the claims

Claim 1 is amended to include the subject matter of claim 2.

Claim 2 is canceled in view of the amendment to claim 1.

Claim 3 is amended to address the rejection under 35 U.S.C. 112 by improving the clarity of the claim language. Claim 3 is also amended along with claim 4 to change the dependency of the claims in view of the cancellation of claim 2.

Claim 16 is amended to include the subject matter of claim 23.

Claim 23 is canceled in view of the amendment to claim 16.

Claim 24 is amended to change its dependency in view of the cancellation of claim 23.

Claim 25 is amended to address the rejection under 35 U.S.C. by changing its dependency from claim 23 to claim 24.

Claim 27 is amended to recite that the reading device is configured such that, for a readout of a first data record contained in a protected storage area of the data carrier, the reading device first reads out a second data record contained in a freely readable storage area of the data carrier and data optically represented on the data carrier. Support for this amendment is found on page 6, paragraph [0032], as originally filed.

It is clear that there is support in the specification for the amendatory language; thus, no new matter is added by these amendments.

Entry of the Amendment to the claims is respectfully requested in the next Office action.

3. Rejection of claims 3, 5 and 25 under 35 U.S.C. § 112

Reconsideration and withdrawal of this rejection is respectfully requested in view of the amendments to claims 3 and 25, as described above. It is submitted that all of the features of the claims are clearly defined.

4. Rejection of claims 1, 7, 9, 15, 16, 18-21, 23, 26, 27, 32 and 33 under 35 U.S.C. § 102(e) as being anticipated by U.S. patent application publication 2003/057276 (*Appalucci*)

Claim 1 is amended to include the subject matter of claim 2. Reconsideration of this rejection with regard to claim 1 is respectfully requested in view of the amendment to claim 1. The Office action acknowledges that *Appalucci* does not teach the subject matter of claim 2. Accordingly, withdrawal of this rejection with respect to claim 1, and claims 7, 9 and 15, which depend from claim 1, is kindly requested.

Reconsideration of this rejection with regard to independent claims 16 and 27 is respectfully requested in view of the amendments to claims 16 and 27, and the following remarks which demonstrate that *Appalucci* does not teach every feature of claims 16 and 27.

In observing amended claim 16, the claim is directed to a method for reliably determining a deliberate use of a contactless data carrier, comprising the step of effecting an optical data transmission with the help of data disposed on the data carrier, wherein for a readout of a first data record, in a first step the reading device reads out a second data record, which is allocated to the first data record, and data optically represented on the data carrier.

In other words, before the first data record can be read by the reading device, the reading device first reads both a second data record which is allocated to the first data record and data optically represented on the data carrier.

As described in paragraphs [0031] and [0032], this arrangement requires the reading device 1 to first determine that it is safe to allow the reading of the data record 23 (protected data) by performing an initial step of reading a data record 25 and data 20 optically represented on the data carrier.

Appalucci does not disclose a method for reliably determining a deliberate use of a contactless data carrier, requiring that in order for a readout of a first data record in a first step a reading device reads out a second data record, which is allocated to the first data record, and data optically represented on the data carrier, as required by amended claim 16.

Appalucci discloses an item 10 having a barcode 14 and a radio frequency identification tag 16 (paragraph [0024]). A system includes a barcode scanner 52 and a radio frequency interrogator 56 for reading the barcode and the radio frequency identification tag (paragraph [0027]). The system also includes a comparator 62 for comparing output signals from the barcode scanner 52 and the radio frequency interrogator 56.

The function of the comparator is to determine wither the identity of the item as read by the barcode scanner 52 is the same as the identity of the item as read by the radio frequency interrogator 56. If the comparison is positive, indicating a match, the comparator sends a positive output signal indicating approval (paragraph [0027]).

Appalucci indicates that the radio frequency identification tag 16 is read slightly before, slightly after or simultaneously with the reading of the barcode label 14. Essentially, the radio frequency identification tag and the barcode label are read concurrently (paragraph [0029], lines 16-23). Indeed, in order for the comparator to compare outputs from the barcode scanner 52 and the radio frequency interrogator 56,

both the barcode label 14 and the radio frequency identification tag 16 must first be read by their respective readers 52,56.

In contrast to *Appalucci*, amended claim 16 requires that in order for a readout of a first data record, in a first step a reading device reads out a second data record, which is allocated to the first data record, and data optically represented on the data carrier.

Indeed, as neither the reading of the barcode label 14 nor the radio frequency identification tag 16 in *Appalucci* is conditioned on an initial reading step, *Appalucci* does not disclose a method for reliably determining a deliberate use of a contactless data carrier, requiring that in order for a readout of a first data record, in a first step a reading device reads out a second data record, which is allocated to the first data record, and data optically represented on the data carrier, as recited in amended claim 16.

Amended claim 27 is directed to a reading device for reading a contactless data carrier, comprising means for reading optical data and being configured that, for a readout of a first data record contained in a protected storage area of the data carrier, the reading device first reads out a second data record contained in a freely readable storage area of the data carrier and data optically represented on the data carrier.

It is submitted that *Appalucci* does not disclose a reading device configured such that for reading a first data record contained in a protected storage area of a data carrier, the reading device first reads out a second data record contained in a freely readable storage area of the data carrier and data optically represented on the data carrier, for the same reasons discussed above with regard to claim 16.

In view of these observations, it is respectfully submitted that *Appalucci* fails to anticipate the pending claims of this rejection. Accordingly, withdrawal of this rejection is kindly requested.

Claims 18-21, 23, 26, 32 and 33 are also considered to be patentable as containing all of the elements of claims 16 and 27, as well as for their respective individually recited features.

5. Rejection of claims 2, 4 and 17 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent application publication 2003/057276 (*Appalucci*) in view of U.S. patent application publication 2003/052159 (*Kawan*)

Reconsideration of this rejection is respectfully requested in view of the amendments to independent claim 1, from which the remaining claims in the rejection depend, and the following remarks which demonstrate that the proposed combination of *Appalucci* and *Kawan* fails to render the pending claims *prima facie* obvious.

In observing amended claim 1, the claim is directed to a contactless data carrier with an antenna and a chip, wherein the chip has storage areas including at least one storage area that is freely readable and at least one storage area that is only readable after an authentication of the data carrier and a reading device.

As described in paragraphs [0033] and [0034], an authentication between the reading device 1 and the chip 3 of the data carrier is provided by means of a derived cryptographic key. A cryptographic key which has been derived from a secret master key is stored on the data carrier. The secret master key is stored on the reading device.

To perform the authentication, a cryptographic key is derived by the reading device from the freely readable data record 25 and the optically readable information 20 on the data carrier using the secret master key stored on the reading device. If the cryptographic key stored on the data carrier is identical to the cryptographic key derived by the reading device, a positive authentication is indicated.

The proposed combination of *Appalucci* and *Kawan* does not disclose a contactless data carrier with an antenna and a chip, wherein the chip has at least one

storage area that is only readable after an authentication of the data carrier and a reading device, as required by amended claim 1.

As discussed above, *Appalucci* discloses an item 10 having a barcode 14 and a radio frequency identification tag 16 which are read by a system including a barcode scanner 52 and a radio frequency interrogator 56 (paragraph [0024]). The rejection acknowledges that *Appalucci* does not disclose a chip having at least one storage area that is only readable after an authentication of the data carrier and a reading device. The rejection turns to the *Kawan* patent to cure the deficiencies of *Appalucci*.

The rejection asserts that the decryption of data stored on a memory card in *Kawan* is a teaching of an authentication. Applicant respectfully disagrees with this assertion. *Kawan* discloses an apparatus for reading from and writing to a multi-memory card (paragraph [0023]). The rejection particularly relies on paragraphs [0030], [0031] and [0043] for the teaching of an authentication. However, these paragraphs merely indicate that a decryption key can be generated from the chip memory and used to encrypt data that is put on an optical strip.

It is first noted that authentication and decryption are completely different functions that serve different purposes and are carried out in different manners. An authentication serves to establish or prove something as genuine (Dictionary.com website). Decryption is merely a process of decoding or deciphering information (Dictionary.com website).

Indeed, there is absolutely no teaching in *Kawan* of an authentication between a data carrier and a reading device, as recited in amended claim 1. In paragraph [0030], *Kawan* indicates that a decryption key is generated from the chip memory and is used to encrypt data that is put on the optical strip. *Kawan* does not provide a discussion of the decryption process.

However, Applicant considers that the same key used to encrypt the data is likely used to decrypt the data (especially since *Kawan* refers to the key used to encrypt the data as a decryption key).

As such, the memory card stores the key and the data encrypted and decrypted by the key, while the reading apparatus does not store any key and merely performs the encrypting and writing steps by means of the key stored on the memory card. It is noted that *Kawan* does not even indicate that the disclosed reading apparatus actually performs the decryption. However, even if the reading apparatus performs the decryption, the apparatus would just reread the key from the chip of the memory card.

This process is clearly not an authentication between the memory card and the reading apparatus, since the reading apparatus does not store any data to be authenticated with the memory card. Therefore, any reading apparatus that is capable of reading the memory card could perform the process disclosed in *Kawan*.

As such, even if *Appalucci* was modified to include the encryption/decryption process of *Kawan*, the resultant device still would not include a data carrier with a chip having at least one storage area that is only readable after an authentication of the data carrier and a reading device.

Therefore, the proposed combination of *Appalucci* and *Kawan* does not disclose a contactless data carrier with an antenna and a chip, wherein the chip has at least one storage area that is only readable after an authentication of the data carrier and a reading device, as recited in amended claim 1.

In view of these observations, it is respectfully submitted that the proposed combination of *Appalucci* and *Kawan* fails to render the pending claims of this rejection *prima facie* obvious. Accordingly, withdrawal of this rejection is kindly requested.

Claims 4 and 17 are also considered to be patentable as containing all of the elements of claims 1 and 16, as well as for their respective individually recited features.

6. Rejection of claims 6, 12, 28, 30 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent application publication 2003/057276 (*Appalucci*) in view of U.S. patent 5,874,724 (*Cato*)

Rejection of claims 8 and 31 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent application publication 2003/057276 (*Appalucci*)

Rejection of claim 14 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent application publication 2003/057276 (*Appalucci*) in view of U.S. patent application publication (*Welte*)

Rejection of claim 29 under 35 U.S.C. § 103(a) as being unpatentable over U.S. patent application publication 2003/057276 (*Appalucci*) in view of U.S. patent 5,789,733 (*Jachimowicz*)

Reconsideration of these rejections is respectfully requested in light of the observations noted above and the amendment to independent claims 1 and 27, from which claims 6, 8, 12, 14 and 28-31 depend.

It is submitted that claims 6, 8, 12, 14 and 28-31 are patentable at least in view of their dependency from claims 1 and 27, as well as for their respective individually recited features.

It is further submitted that *Cato*, *Welte* and *Jachimowicz*_ do not make up for the shortcomings of *Appalucci*. Accordingly, withdrawal of these rejectios is respectfully requested.

7. Conclusion

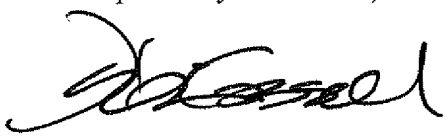
As a result of the amendment to the claims, and further in view of the foregoing remarks, it is respectfully submitted that the application is in condition for allowance. Accordingly, it is respectfully requested that every pending claim in the present application be allowed and the application be passed to issue.

If any issues remain that may be resolved by a telephone or facsimile communication with the applicants' attorney, the examiner is invited to contact the undersigned at the numbers shown below.

BACON & THOMAS, PLLC
625 Slaters Lane, Fourth Floor
Alexandria, Virginia 22314-1176
Phone: (703) 683-0500
Facsimile: (703) 683-1080

Date: October 13, 2009

Respectfully submitted,



JUSTIN J. CASSELL
Attorney for Applicants
Registration No. 46,205

Related Searches

Decryption programs
Encryption decrypti...
Download decryption...
Free css decryption...
Dvd decryption
Decryption tools
Decrypt
Free dvd decrypter ...
Decryption hacking ...
Password decryption
Free dvd decryptor
Encryption decrypti...

Nearby Words

decrustation
decry
decrypt
decryption
decstation
dect
dectape

decryption - 3 dictionary results

de·crypt [dee-**kript**, di-] Show IPA

–verb (used with object)
to decode or decipher.

Origin:
1935–40; DE- + CRYPT(OGRAM)

Related forms:
de·cryp·tion, noun

Dictionary.com Unabridged
Based on the Random House Dictionary, © Random House, Inc. 2009.
Cite This Source | Link To decryption

NEW Related Words for : **decryption**
decipherment, decoding
View more related words »

VISUALTHESAURUS
decryption
Explore the Visual Thesaurus »

de·crypt (dē-krĭpt')
tr.v. **de·crypt·ed, de·crypt·ing, de·crypts**
1. To decipher.
2. To decode.

n. (dē'krĭpt')
A deciphered or decoded message.

[**de-** + **-crypt** (from **cryptogram**).]
de·cryp'tion *n.*

The American Heritage® Dictionary of the English Language, Fourth Edition
Copyright © 2009 by Houghton Mifflin Company.
Published by Houghton Mifflin Company. All rights reserved.
Cite This Source

Unscramble a synonym of decryption

decryption ***cryptography***
Any procedure used in cryptography to convert ciphertext (encrypted

(1995-05-10)

authentication Search

Related Searches

User authentication
Network authenticat...
User authentication...
Autograph authentic...
Kerberos
Authenticate an aut...
Authentication of u...
Authentication prot...
Autograph authentic...
Types of authentica...
Introduction to aut...
Global authenticati...

Synonyms

attestation
validation
proof
testimonial
warrant
corroboration
demonstration
More Synonyms »

Nearby Words

authentical
authenticatable
authenticate
authentication
authenticator
authenticity
authigenic

authentication - 4 dictionary results

au·then·ti·cate [aw-**then**-tl-keyt] Show IPA

–verb (used with object), -cat ed, -cat ing.

1. to establish as genuine.
2. to establish the authorship or origin of conclusively or unquestionably, chiefly by the techniques of scholarship: *to authenticate a painting.*
3. to make authoritative or valid.

Origin:
1565–75; < ML *authenticātus* made authentic (ptp. of *authenticāre*). See AUTHENTIC, -ATE 1

Related forms:
au thenti cat a ble, adjective
au thenti ca tion, noun

Synonyms:
1. confirm, validate, substantiate.

Related Words for : **authentication**
assay-mark, hallmark, certification
View more related words »

Explore the Visual Thesaurus »

au·then·ti·cate (ô-thĕn'tĭ-kāt') tr.v. **au·then·ti·cat·ed, au·then·ti·cat·ing, au·then·ti·cates**
To establish the authenticity of; prove genuine: *a specialist who authenticated the antique samovar.* See Synonyms at confirm.
au·then'ti·ca'tion *n.*, **au·then'ti·ca'tor** *n.*

Unscramble a synonym of authentication

Legal Dictionary

Function: *transitive verb*
Inflected Forms: **-cat·ed; -cat·ing**
1 : to prove or serve to prove that (something) is genuine; *especially* : to prove that (an item of evidence) is genuine for the purpose of establishing admissibility
2 : to make (a written instrument) valid and effective by marking esp. with one's signature <*authenticate* a check>

Merriam-Webster's Dictionary of Law, © 1996 Merriam-Webster, Inc.
Cite This Source

Computing Dictionary

authentication ***security***
The verification of the identity of a person or process. In a communication system, authentication verifies that messages really come from their stated source, like the signature on a (paper) letter. The most common form of authentication is typing a user name (which may be widely known or easily guessable) and a corresponding password that is presumed to be known only to the individual being authenticated. Another form of authentication is biometrics.
(2007-02-22)

The Free On-line Dictionary of Computing, © 1993-2007 Denis Howe
Cite This Source

Search another word or see **authentication** on Thesaurus | Reference